The Ordo host based scanner.

Brett Viren

Physics Department

BROOKHAVEN NATIONAL LABORATORY

The Ordo Host Base Configuration Assessment Tool

outline

1. What is Ordo?

2. Why do we need Ordo?

3. Installation

4. Summary

overview

The Ordo configuration assessment and asset management suite

- Name comes from the Latin "Novus Ordo Seclorum" ("New Order of the Ages")
- Collaborative effort by ITD (Rich Casella) and Physics (bv).
- Consists of:
  1. Host based client "ordo" gathers data
  2. Central "master" receives data
  3. Backend Oracle database stores data
  4. Web based report and remediation pages
- Running the ordo client on unix-like computers is a **requirement** if connecting to the internal network.

client

- Works on unix-like systems (currently AIX, Debian, FreeBSD, Gentoo, Mac OS X, Mandrake, Redhat IRIX, Slackware, Sun)
- Implemented in modular Perl, minimal system requirements.
- Communicates with master through SMTP.
- Runs from cron
  - fast scans hourly, full scans daily.
  - no change ⇒ only small heartbeat message sent.
  - self updating, source code is signed by master's PGP key.
- Focus on security:
  - No listening daemons. Source code and data open to sysadmins.
  - Comunication is cryptographically signed and encrypted.
  - Requires (mostly) no elevated privileges
  - Operates in read-only mode. System not modified.

modular client

- The client implements each test as a cascade of procedures:
  1. Platform-independent Ordo client code.
  2. Platform-specific Ordo client code.
  3. Host-dependent external “helper” program. Sysadmin can override any test by providing their own “helper” program in `helpers/` sub directory.
- New tests can be easily “plugged in”.
- Several scan types: “full”, “fast” and “fake” (no mail message sent).
- Not all tests are currently supported on all platforms. Need help here.

scans

- Host fingerprint (uname, distribution/vendor)
- List of users
- Network interfaces
- System packages and their versions
- Various `/etc` config files
- Set UID root files
- World writable files
- Other CIS benchmarks
- Passwords for cracking (may need suid-root binary)
- Others...

Soliciting volunteers to help write missing tests.

scan data example

```
{
  "nic" => {
    "test" => "NIC",
    "timestamp" => "1142027537",
    "version" => "1.4",
    "status" => "okay",
    "args" => "",
    "name" => "nic",
    "data" => {
      "lo.0" => {
        "ip" => "127.0.0.1",
        "status" => "UP",
        "iface" => "lo",
        "mac" => "",
        "mask" => "255.0.0.0"
      },
```

```
"eth0.0" => {
        "ip" => "130.199.36.108",
        "status" => "UP",
        "iface" => "eth0",
        "mac" => "00:E0:81:05:43:CE"
        "mask" => "255.255.254.0"
      },
      "eth1.0" => {
        "ip" => "",
        "status" => "DOWN",
        "iface" => "eth1",
        "mac" => "00:E0:81:05:43:CF"
        "mask" => ""
      }
    }
  },
{more tests...},
}
```

why?

Why Ordo?

- Part of FISMA requires that we assess the configuration of our systems.
- Regular, manual assessment too labor intensive.
- Attempted to use SLAC's Ranger tool. Rejected due to lack of needed features and code complexity.
- DOE has purchased a proprietary Radia-like tool ("Hercules"). Some concerns over its use. Hopefully Ordo can supplant it at BNL.

deployment status

Current Ordo deployment:

Redhat	354
Debian	119
Sun	42
Mac	32
SGI	5
AIX	2
Gentoo	2
Mandrake	2
FreeBSD	1
Slackware	1
Total	560

Still to do:

- 1842 Physics cluster nodes
- 415 Physics workstations (1005 lab wide)
- 277 Physics servers (373 lab wide)

Target for finished deployment is end of this month.

interactive installation

```
root# useradd -u 111 -d /var/lib/ordo -c "Ordo Scanner" -m ordo
root# su - ordo
ordo$ wget http://ordo.bnl.gov/downloads/client/ordo.latest.tar
ordo$ tar xf ordo.latest.tar
ordo$ client/ordo-init
(answer interactive questions)

ordo$ client/ordo chkstatus
```

Last command is optional, will return a summary of the master's view of your system.
Detailed instructions available at http://ordo.bnl.gov/

batch installation

The `ordo-init` can be run with answers supplied by environment variables.

ORDO_BASE where the client expects to find the Perl source code and working directories.

ORDO_PERL the full path to the Perl interpreter. ordo-init tries to locate this by checking a few conventional locations.

ORDO_GPGBIN the full path to the GnuPG "gpg" executable.

ORDO_NAME a common name for the Ordo client user to use when generating the GPG keys.

ORDO_EMAIL the email address to use when generating the GPG keys.

ORDO_SMTP_SERVER the email server that can relay the messages.

ORDO_SECRET the client's "secret" GPG passphrase.

demo

summary

- The Ordo host based configuration scanner built in-house.
- Required for unix-like systems on the internal network.
- We have this month to deploy it.
- Contact Rich Casella `<rac@bnl.gov>` or Brett Viren `<bv@bnl.gov>` with problems, any special concerns or if you want to help out.